WHITE PAPER

The Need for Enterprise-Grade File Sharing and Synchronization

An Osterman Research White Paper

Published August 2012

SPONSORED BY

Accellion

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

OSTERMANRESEARCH

EXECUTIVE SUMMARY

Cloud-based file-sharing and synchronization (FSS) tools are among the hottest applications used in the workplace, offered by market-leader Dropbox, Inc. and a large and growing number of vendors. These tools, which broadly can be classified as "consumer-focused" because they are typically deployed by individual users and not as part of a coordinated IT plan, offer tremendous usability. By synchronizing files across a variety of platforms – desktop, laptop, smartphone and tablet – these tools enable users to have near real time access to all of their content from any computing platform and any location.

However, these tools create a number of problems for IT and organizations in general:

- Files that are shared and stored on individual platforms – many of which are personally owned devices like smartphones and tablets – are normally not managed in accordance with IT compliance and governance policies. This means that files may not be encrypted, backed up or archived as files on IT-managed systems would be.

- The vendors who manage the cloud data centers in which customer files are stored may or may not provide sufficiently robust security to protect content from unauthorized access, malware infection or inadvertent data leakage.

- Files shared using these tools are often not scanned by corporate malware systems, and so create an additional opportunity for malware to enter the corporate network.

- FSS tools have been used on some occasions to distribute spam.

- FSS tools can also create other problems, including the mixing of corporate and personal data – leading to privacy problems in some cases – and they can also complicate the e-discovery and regulatory management process.

Files that are shared and stored on individual platforms – many of which are personally owned devices like smartphones and tablets – are normally not managed in accordance with IT compliance and governance policies.

KEY TAKEAWAYS

- FSS tools are extremely useful and they make users more productive because they enable access to content in near real time on a variety of devices.

- However, these tools create serious compliance, governance and security problems. Our research found that 49% of organizations believe the problems created by these tools are about as serious as they were 12 months ago, but 42% report they are more serious – only 8% find they are now less of a problem.

- In response, IT departments should *not* establish policies or take other measures to *prevent* the use of file synchronization capabilities per se. Instead, IT departments should deploy enterprise-grade replacements for these tools that will provide the same benefits of everywhere-access to files, but that put IT in control of the content that is shared using these files.

AN IMPORTANT CAVEAT

Throughout this white paper we refer to "consumer-grade" FSS tools and "Dropbox" (referring to the solutions offered by Dropbox, Inc.). It is important to note that our purpose in this white paper is not to denigrate either this category of tools or Dropbox in particular, but rather to provide a fair and honest assessment of these tools' benefits and drawbacks.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Accellion – information about the company is offered at the end of this white paper.

THE CURRENT STATE OF FILE SHARING AND SYNCHRONIZATION

USERS NEED TO SHARE AND SYNCHRONIZE CONTENT

One of the fundamental tenets of the modern enterprise is that users need to share information with others for a variety of purposes: to collaborate on the creation of documents, presentations and spreadsheets; to send, sign or receive critical business documents like proposals, contracts and purchase orders; and to broadcast content of various types.

Moreover, users need to synchronize content across the growing variety of platforms they use to create, view and share content. For example, it is not uncommon for a user to create a document on a desktop computer, modify it on a laptop while traveling or at home after hours, view it on a tablet, and share it with someone else using a smartphone.

Another important driver for the need to have anywhere-access to content is permanent or semi-permanent telecommuting in which users do not have an office, but instead work from home, going into an office only when necessary. For example, 40% of IBM employees work remotely[i] and 85% of Cisco's employees telecommute[ii] on a regular basis. IDC estimates that more than three million corporate office home offices will be added to the current base of US teleworking households between 2011 and 2015[iii]. Add to this the majority of information workers that work at home or otherwise remotely after hours and must have access to content. This out-of-office experience further drives the need to have access to the same documents – and the correct versions of these documents – available in a variety of locations and on several different devices.

EMAIL IS USEFUL FOR COMMUNICATION, BUT NOT SO USEFUL FOR COLLABORATION

Email has become the de facto tool for sharing content with others because of its ease of use, the fact that it is universally accessible because it is built on industry standards, and it is available from virtually any computing platform. However, email has some serious shortcomings as a file-sharing tool: it is cumbersome to use for content synchronization, it contributes to version control problems, and most corporate email administrators place limits on the maximum size of a file that can be sent using email.

Email has some serious shortcomings as a file-sharing tool: it is cumbersome to use for content synchronization, it contributes to version control problems, and most corporate email administrators place limits on the maximum size of a file that can be sent using email.

To overcome the limitations with email, many users employ FTP systems, personal Webmail or physical delivery. However, these alternatives introduce their own set of limitations:

- FTP systems require IT to provision and manage these systems, not to mention the fact that undermanaged FTP servers can store content for years and lead to potentially unauthorized access to sensitive content.

- Personal Webmail bypasses corporate content scanning, archiving and backup procedures, not to mention the fact that corporate files are stored outside of the company's control or access.

- Physical delivery or transport of content, such as on CDs/DVDs or USB sticks, is slow, cumbersome and expensive. Moreover, when users copy files to a USB stick to take work home with them, they can run into version control issues, they may forget particular files they need to do their work, they may infect corporate files when using them on an unprotected home PC, or they may lose the USB stick and sensitive corporate data with it.

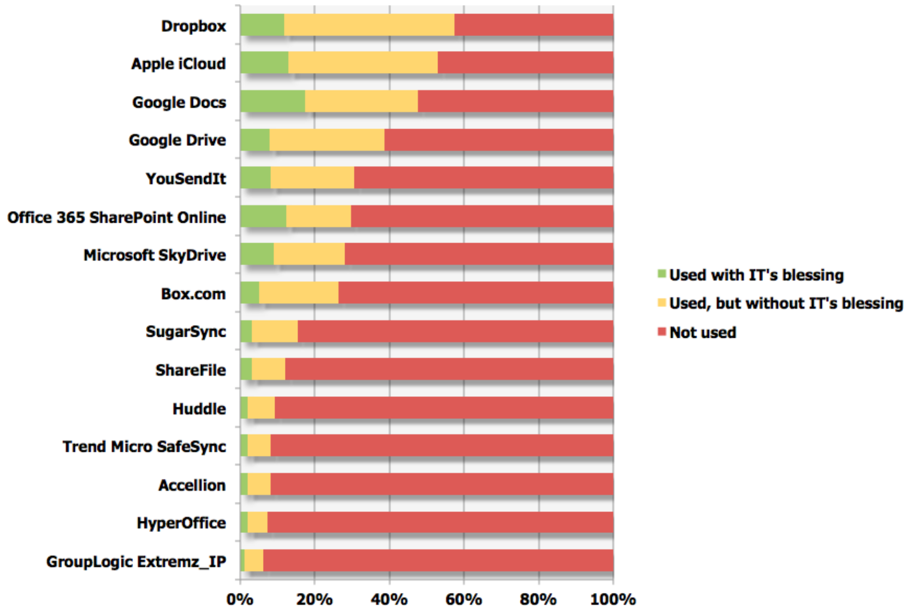
DROPBOX HAS BECOME THE DE FACTO STANDARD FOR CONTENT SYNCHRONIZATION

To satisfy their content-sharing and synchronization requirements, millions of users have turned to FSS tools, most of which use a) a client installed on each device and b) the cloud for synchronization of content. These tools, most of which are available for free or at a nominal cost, are extremely easy to use and work exactly as advertised: they allow content created or saved on one device to be distributed to, or at least easily accessible from, any other device a user employs.

Dropbox has become the leading FSS tool with a user base exceeding 50 million users as of Spring 2012[iv], up from just 3 million users two-and-a-half years earlier[v]. Although Dropbox is the clear market leader, there are many other file synchronization tools in use from a large and growing number of vendors. An Osterman Research survey conducted specifically for this white paper found a large number of FSS tools in use in the workplace – most consumer-focused and a few true enterprise-grade tools. Moreover, some of these tools are used with IT's blessing, but most are used without it.

Roughly one out of every 16 corporate files is stored in a primarily consumer-focused file-sharing and synchronization system.

File Synchronization Tools in Use With and Without IT's Blessing
As a % of Organizations



To underscore just how important these tools have become, our research discovered that among those respondents who could estimate the total amount of their corporate data that is managed using FSS tools, the average was 6.2% -- i.e., roughly one out of every 16 corporate files is stored in a primarily consumer-focused FSS system. However, 39% of respondents have no idea how much of their data is stored in the systems.

WHY ARE THESE TOOLS USED?

The vast majority of corporate employees are smart and they want to find effective and efficient ways of doing their work. As a result, users are increasingly turning to FSS tools because of the many benefits they offer:

- They eliminate the file size limitations inherent in email.

- They are much easier to learn and use than FTP systems. In fact, once the local client software has been installed, file synchronization takes place automatically and transparently such that simply saving a file makes it accessible within seconds on other platforms, either for personal use or sharing with others.

- These tools make bringing work home or on the road far simpler and more reliable.

- These tools are available at very low cost. Most providers offer two or more gigabytes of storage at no charge, with much larger amounts of storage available for a nominal monthly fee.

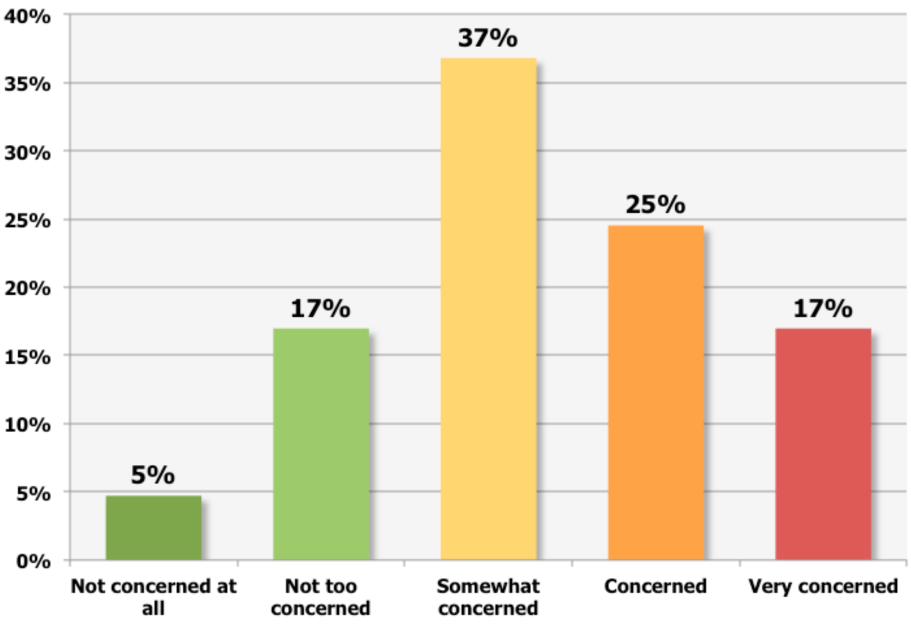
The bottom line is that FSS tools combine ease-of-use, low cost and utility that more traditional file-sharing technologies simply cannot match in terms of cost or convenience.

PROBLEMS WITH THE STATUS QUO

Despite the many benefits of the consumer-focused FSS tools in use in the workplace today, there are a variety of problems that these tools introduce, as discussed below. The magnitude of these problems has not been lost on decision makers: as shown in the following figure, nearly four out of five organizations surveyed for this white paper are at least somewhat concerned about these problems.

When content is shared using consumer-focused file-sharing and synchronization tools, content is normally not encrypted unless the user specifically chooses to do so and installs additional software for this purpose.

IT Management Concern About the Use of Consumer-Grade File Sharing and Synchronization Solutions



SO, WHAT ARE THE PROBLEMS?

There are four fundamental issues associated with the use of consumer-focused FSS tools in a workplace context:

- **A lack of compliance and governance capabilities**
  When content is shared using consumer-focused FSS tools, content is normally not encrypted unless the user specifically chooses to do so and installs additional software for this purpose. The result is that potentially sensitive corporate data

can be sent over the Internet and stored in a third party's cloud data center without encryption, potentially exposing it to interception and possibly in violation of regulatory obligations (e.g., the Health Insurance Portability and Accountability Act [HIPAA] or the Payment Card Industry Data Security Standards [PCI DSS]). For example, Dropbox encrypts customer data on the server side, but not at the client.

Moreover, when content is stored in a cloud-based FSS vendor's data center, accessing this data for purposes of e-discovery or a regulatory audit becomes impractical or impossible because of the need for IT to gain access to every such account and then search it for the required content. Plus, tools like Dropbox are not compliant with a number of compliance standards like HIPAA, PCI DSS, ISO 27001, ISO 9001 or the Family Educational Rights and Privacy Act (FERPA).

Finally, most consumer-focused file synchronization services do not permit users to control the physical location of data, which can lead to regulatory problems or others issues in jurisdictions that require sensitive data to be stored only in certain geographies, or at least make it desirable to do so. For example, a non-US company will typically prefer that its data not be stored in a US-based data center to avoid its access under the PATRIOT Act. Some types of data held by countries in the EU are required to store data only in certain geographies.

- **A lack of IT control over content**
  Another serious shortcoming of most consumer-focused FSS solutions is that they provide IT with no control over the lifecycle of data sent using these solutions. For example, these tools typically do not provide any control over when content will expire and thus will no longer be viewable, they provide no policy-managed encryption, and they do not provide any policy-managed permissions or access control. More fundamentally, corporate policies that control encryption, backup, archiving or DLP that apply to content sent through email or FTP systems cannot be applied to content sent through consumer-focused FSS tools. In short, the lack of IT control over the content sent through most FSS tools puts the employee in charge of employer-owned data, when in reality it should be the latter.

  Related to IT's lack of control over content when employees use file synchronization tools is that not all cloud providers offer a stellar record of security protection. For example, on June 19, 2011, Dropbox experienced a serious security breach for three hours and fifty-two minutes that permitted anyone to access customer-owned data[vi].

- **An inability to scan content for malware**
  Another shortcoming of consumer-focused FSS tools is that they typically do not scan content for unwanted content like malware or spam. This permits content from an unprotected home computer, for example, to be infected with malware, uploaded to the cloud, and then downloaded to a user's work computer, circumventing corporate malware-scanning systems and potentially spreading the infection throughout a company's network. Dropbox, for example, admits that it does not scan for malware: in a February 2012 forum post, a Dropbox moderator noted that "Checking [for malware] will only be done on your own machine after it has downloaded.[vii]"

  Although not common, Dropbox has also been used to distribute spam. Symantec, for example, found that Dropbox has been used to distribute spam[viii].

- **A mix of corporate and personal data**
  Another problem with consumer-focused FSS tools – because they are normally under the control of end users – is that they can be used to send and share a mix of corporate and personal content. For example, mixed with sensitive company information might be an employee's vacation photos, résumé or personal financial records. This makes activities like e-discovery or regulatory

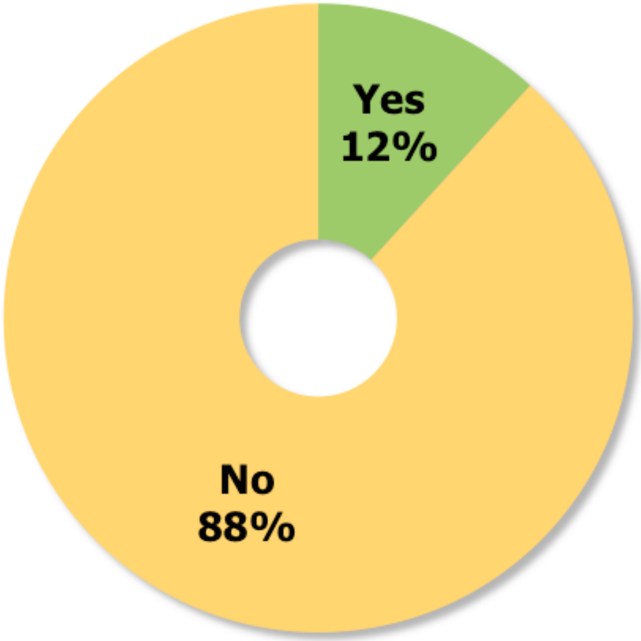
A serious shortcoming of most consumer-focused file-sharing and synchronization solutions is that they provide IT with no control over the lifecycle of data sent using these solutions.

compliance much more difficult because reviewers will often find, and must sort through, personal data as they search for corporate records that are relevant to the discovery process. Moreover, privacy rights for personal data might become a thorny issue, particularly in jurisdictions that are heavily focused on employee privacy rights.

The bottom line is that use of most consumer-focused FSS tools put organizations at greater risk and it drives up the overall cost of managing corporate data assets and networks. Complicating the issue further is that while most organizations use consumer-focused FSS tools, most do not use their enterprise-grade equivalents, as shown in the following figure.

Use of most consumer-focused file-sharing and synchronization tools put organizations at greater risk and it drives up the overall cost of managing corporate data assets and networks.

"Does your company use enterprise-grade cloud file synchronization solutions?"

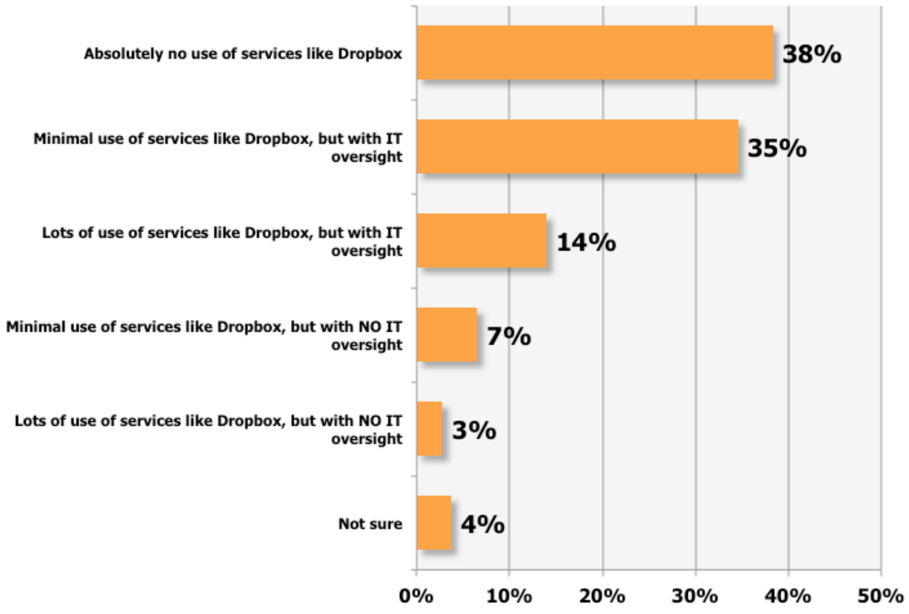


It is also important to note that our research found 45% of users in the organizations surveyed currently use mobile apps to access cloud-based FSS tools, but only 18% of organizations currently support these mobile apps.

YOUR OPTIONS TO GAIN THE UPPER HAND

Many IT decision makers and influencers would prefer that Dropbox and other types of consumer-focused file synchronization tools not be used at all. As shown in the following figure, a plurality would prefer that these tools not be used (not surprising given the problems they can cause), while about one-half want varying levels of use, but with IT oversight of the data sent and stored in these services.

"What would your IT management prefer for services like Dropbox?"



WHAT SHOULD YOU DO?

Decision makers faced with the prospect of users who have installed and are using consumer-focused FSS tools – i.e., most organizations – have three options to deal with the problem:

- **Do nothing**
  This is clearly the simplest and least expensive option for decision makers to consider. However, it also is the most risky option from a compliance, IT control and security perspective for the reasons noted above. Osterman Research highly recommends that the "Do Nothing" approach not be considered.

- **Create policies that require users not to employ these tools**
  Another relatively simple option is to implement a corporate policy that requires employees not to install or use any sort of consumer-focused FSS tool. While some employees will comply with the policy, it is safe to assume that many will not. For example, a 2011 Osterman Research survey asked 214 IT decision makers and influencers about their level of agreement with the statement, "[Our] employees do not install applications on their computers in violation of IT policies". The survey found that 30% of respondents in organizations of up to 500 employees disagreed or strongly disagreed with this statement; in larger organizations the situation was even worse: 41% disagreed or strongly disagreed. Clearly, policies will not be an effective method to prevent the download and installation of consumer-focused FSS tools.

- **Deploy an enterprise-grade file synchronization tool**
  Osterman Research highly recommends the deployment of an enterprise-grade FSS tool as a replacement for the consumer-grade equivalents that are so prevalent in most organizations today. Doing so will offer the best of both worlds: it will give users the flexibility and ease of use that drives them to consumer-focused file sharing and synchronization; and it will give IT easy access to corporate data when required, the ability to control how content is sent, and where it is stored.

  Key features of an enterprise-grade solution should include:

Osterman Research highly recommends the deployment of an enterprise-grade file-sharing and synchronization tool as a replacement for the consumer-grade equivalents that are so prevalent in most organizations today.

- The ability for users to synchronize content easily
- The ability for IT to easily deploy and manage the system
- Access using a variety of devices, browsers and operating systems
- Integration with LDAP or Active Directory
- In some cases, deployment on-premise if IT prefers this approach
- Tracking of all file versions
- The ability to stored deleted files, if desired
- Activity logs to monitor content flows
- Encryption of sensitive content
- Management of content according to corporate policies
- The ability to archive content
- Permission and access control for individual files
- The ability to establish expiration periods for files
- A complete audit trail for compliance purposes

SUMMARY

Consumer-focused FSS tools provide enormous benefits to end users, but they introduce a number of risks and other problems in a corporate setting. Consequently, every organization should deploy an enterprise-grade FSS tool that will combine the benefits of their consumer-focused equivalents with the IT control that organizations require.

SPONSOR OF THIS WHITE PAPER

Accellion, Inc. provides enterprise-class mobile file sharing solutions that enable secure anytime, anywhere access to information while ensuring enterprise security and compliance. The world's leading corporations and government agencies use Accellion to protect intellectual property, ensure compliance, improve business productivity and reduce IT costs.

Founded in 1999, Accellion file sharing solutions can be deployed on public, private and hybrid cloud environments and provide the ease-of-use business users need while giving the enterprise organization the flexibility, scalability and protection it needs.

Accellion is a profitable, well-funded, private company with more than 10 million users and 1,500 enterprise organizations that have deployed Accellion with a more than 96 percent annual renewal rate. Current customers include Procter & Gamble; Activision; Indiana University Health; Kaiser Permanente; Foley & Mansfield; Lovells; Bridgestone; Ogilvy & Mather; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA.

For more information please visit www.accellion.com or call (650) 485-4300.

Connect with Accellion:
Web: http://www.accellion.com
Twitter: http://www.twitter.com/accellion
Facebook: http://www.facebook.com/accellion
LinkedIn: http://www.linkedin.com/companies/accellion

Accellion®

www.accellion.com
twitter.com/accellion
info@accellion.com

+1 855 485 4300
+1 650 485 4300

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statue, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

[i] http://www.ibm.com/ibm/responsibility/employees_well_being.shtml

[ii] http://www.vancouversun.com/jobs/Welcome+workplace/5772250/story.html

[iii] *U.S. Home Office 2011–2015 Forecast: Recovery Drives Interest in IT as Home Office Households Adjust to New Economic Realities,* International Data Corporation

[iv] http://www.dropbox.com/static/docs/DropboxFactSheet.pdf

[v] http://gigaom.com/2009/11/24/dropbox-raises-7-25m-crosses-3m-users/

[vi] http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/

[vii] http://forums.dropbox.com/topic.php?id=52598

[viii] http://www.symantec.com/connect/blogs/dropbox-abused-spammers-0